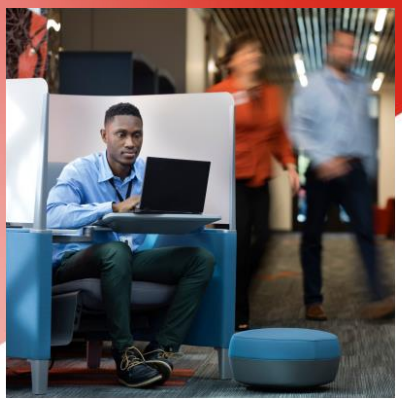
DOC2133

W. L. GORE & ASSOCIATES

ACCEPTABLE USE POLICY

For Gore Partners



Introduction

Gore Assets provide us with the capability to do business with our customers, Partners, and each other. At Gore, we believe that Associates and Partners act in a responsible manner and demonstrate due care to protect our Assets when conducting business. This Acceptable Use Policy and our commitment to meeting its requirements is critical to our success as an Enterprise.

Purpose

The purpose of this Acceptable Use Policy ("Policy") is to set forth the responsibilities of Gore Partners who access or use W. L. Gore & Associates ("Gore" or "the Company") Assets. This Policy is in place to protect Gore's Information Resources and guide Gore Partners in the appropriate use of those resources.

This Policy shall supersede and replace the prior AUP. Gore Partners shall sign this Policy to acknowledge they have read, understood, and agreed to comply with the contents set forth in this document.

Scope

This Policy applies to all Gore Partners who use Gore Assets.

All use of Gore Information Resources or access to Gore information, whether on Company issued hardware, a personally owned managed device or on a personally owned unmanaged device (subject to approval) is subject to this policy.

Omission from this Policy does not necessarily constitute permission. If you have any questions regarding an area not covered by this Policy or a potential conflict, please contact your Gore Guide or ITAC.

Definitions

Definitions pertinent to this policy are outlined below. See the Enterprise IT Glossary for additional definitions.

AI Tools – any software application that utilizes artificial intelligence algorithms to perform specific tasks and solve problems. AI Tools include, but are not limited to:

- *Machine Learning Tools (ML),* that analyze data to identify patterns and make predictions, helping Gore with tasks like demand forecasting, customer segmentation, and fraud detection.
- *Natural Language Processing Tools (NLP),* that process and analyze human language, enabling applications like chatbots, sentiment analysis, and automated customer support.
- *Computer Vision Tools,* which allow computers to interpret and make decisions based on visual data, useful in areas like quality control, facial recognition, and automated inspections.
- *Robotic Process Automation Tools (RPA),* that automate repetitive tasks, such as data entry and invoice processing.
- *Predictive Analytic Tools,* that use statistical algorithms and machine learning techniques to predict future outcomes based on historical data, aiding in decision-making processes.

- *Generative AI like Large Language Models (LLM),* that generate content, such as text, images, or code, based on input data, which can be used for content creation, marketing, and more.
- Application with *Retrieval Augmented Generation (RAG),* that generates content with personal data, while this data does not originate from the AI model itself, but from the input, be it from the Associate's prompt or other data sources consulted.
- *Translation Management Systems (TMS),* that leverage automation and may incorporate some AI elements to enhance translation workflow, such as checking for previous translations and integrating new content into the original document layout.

Assets - any hardware or software (Gore issued or Gore managed), or other component of the Gore environment that supports business operations and is owned, licensed, used or operated by Gore.

- *Hardware* includes but is not limited to computers, laptops, tablets, computer hard drives, network hardware, flash drives and other storage devices, workstations, telephones, mobile devices, video conferencing equipment, printers, scanners, and/or any other physical technology that supports business operations.
- *Software* includes but is not limited to operating systems, networking software, messaging applications, as e-mail, voicemail, collaboration tools, word processing, spreadsheet and other data applications, databases, web applications, and/or any other program, application, or software platform.

Content - Data, information, or records that have value to the business based on operational, legal, or regulatory needs.

Data - Content that is a symbolic representation of something that depends, in part, on its metadata for its meaning. Data is a collection of facts, such as numbers, words, measurements, observations, or descriptions of things.

Data Protection Officer - The General Data Protection Regulation (GDPR) has established the concept of a Data Protection Officer (DPO) in Europe. A DPO is working towards compliance with all relevant data protection laws, monitoring specific processes and collaborating with the respective supervisory authorities.

Gore Email Account - A user account (including software, storage, and hardware) associated with a Gore domain that allows you to send and receive email.

Information - Content with short-term business value. Information is data in context.

Internet Access - All resources that enable electronic communication, particularly the retrieval of data from the internet, including the related hardware and software.

Intranet – All resources provided by Gore that allow electronic communication on Gore's **internal** network including the related hardware and software.

Records – Content that is evidence of business actions, decisions, or transactions. Records are complete and finalized information in any format (paper or electronic) that must be retained for defined periods of time based on legal, regulatory, or operational requirements.

Managed Device – Personal mobile devices used to access Gore content or the Gore

network, that have Gore device management software installed and enabled.

- See Mobile Device Use Guidelines

Partner – contractors, third-party, etc.

Use of Gore Assets

Gore business must be conducted through approved applications or managed devices. Not doing so creates risk that Gore content is not appropriately maintained and is less secure.

It is the responsibility of every Gore Partner to keep Gore content secure and not allow access to any Asset unless they are an authorized Associate or Partner.

Access

Gore Partners should only use those Assets to which they have been granted access.

Gore Partners shall take the following steps when accessing or granting access to Gore Assets:

- Gore Partners should access or grant access to Gore assets using the "Need-to-Know" principle.
- Gore Partners should grant access to Gore assets only for as long as necessary and revoke access when business requirements have been met or there is a change to commitment.
- When necessary, Gore Partners must request access through appropriate channels (Application Owner, Information Security, etc.).
- Remote access to the Gore network is permitted only through Gore authorized methods and devices.

Handling

Gore Partners should manage Gore Assets in a secure manner by adhering to the guidelines provided in the Security Classification Policy and Records and Information Management Policy.

Prohibited Use

Gore Partners shall not:

- Engage in unlawful or malicious use of Gore Assets, in particular if such use may damage Gore's reputation, cause liability or financial harm to the Company.
- Access, download, display or disseminate material that may be considered obscene, racist, sexist, threatening, offensive, discriminatory, or abusive.
- Use threatening, harassing or abusive language or content.
- Display content that would be deemed inappropriate for the workplace.
- Attempt to circumvent any security mechanisms put in place by Information Security or the Gore Physical Security Team.
- Use another Associate or Partner's login credentials.
- Connect to the Gore network using a personal unmanaged device.
- Set up an unauthorized wireless network in a Gore facility, attached to the Gore network or access an unauthorized wireless network in a Gore facility.
- Install or modify existing Assets or engage in an activity that intentionally compromises or causes a malfunction or failure of Gore Assets.
- Tamper with or disable Gore's anti-virus software or encryption functionality.

- Install personal or non-standard software on a Gore Asset (except personal apps on a smart phone or tablet).
- Store Gore data or information on a personally owned device (computer, phone, cloud storage, etc.) unless the device has Gore software in place to manage the information being stored on said device (see Bring Your Own Device User Agreement) or in a cloud or network that has not been evaluated by Gore Information Security.

Monitoring

Unless prohibited by law, and to ensure compliance with Gore policies and standards, Gore maintains the right to view, intercept, block, log activity, or otherwise investigate ("monitor") any use of Gore Assets, by any Associate or Partner, and potentially without notice.

When monitoring, Gore will employ all reasonable efforts to adhere to country specific laws to ensure Personal Information ("PI") is used only for a stated and particular purpose.

Whenever possible, monitoring is conducted on an automated basis. Certain information will be captured during monitoring. The types of information that may be gathered, under certain circumstances and for specific purposes, can be found in the attached Appendix B.

Gore may monitor, if allowed by applicable local law, for certain sensitive information (i.e., Export Controlled, Personal Information, or Confidential Gore Technology, etc.) to comply with regulations or to protect Gore's brand reputation and protect the Company's competitive advantage.

Other regional procedures or local laws may apply with respect to monitoring. Further information on how this monitoring is carried out for Associates can be found in the attached Appendix A.

To the extent permitted by applicable law, Gore may attempt to identify a Gore Partner if Gore has reason to believe the Gore Partner is violating this Policy or other related policies. It may, after consultation with the appropriate Data Protection Officer, engage in targeted monitoring.

If, through monitoring, Gore suspects there has been a violation of this Policy:

- Gore reserves the right to remove Gore Partner access to Gore Assets. Where appropriate, Gore will also delete or block access to any Company information on personal devices (see Bring Your Own Device User Agreement).
- Subject to applicable law, Gore may store copies of any content captured through monitoring activities that reflect the inappropriate use of Gore Assets by a Gore Partner. Gore may also disclose copies of such content or a device that contains such content, as necessary in the event of litigation or investigation.

Personal Devices

Gore may allow Gore Partners to use personally owned devices, such as smart phones or tablets to conduct Gore-related business. In those cases:

- Gore Partners must sign a User Agreement via ITAC request process and allow Gore IT to install Mobile Device Management software. Mobile Device Management software allows

Gore IT to control Gore content and applications on the device, or
- On a limited basis, access may be granted per the exception process outlined below.

Electronic Communications

The Gore e-mail system and other messaging services such as Teams or other Gore managed instant messaging ("IM") tools and all associated information within those tools is the express property of Gore, unless otherwise governed by a local law or regulation. Gore e-mail and IM accounts are to be used for Company business. In all electronic communications, securing the confidentiality of sensitive and Personal Information (generally through the use of encryption) is required in alignment with our Security Classification Standard.

Messaging Apps

Gore recognizes the need to communicate internally and externally via instant messaging or communications apps. Whenever possible, we highly encourage the use of an app, platform, or tool that is provided and maintained by Gore and used on a Gore-approved device.

If it is necessary to communicate via an external messaging app such as WhatsApp, never transmit confidential or sensitive information, including personal information or intellectual property.

Messaging should be primarily logistical in nature. Never store Gore business records in any instant message or messaging app. All business records, such as approvals and transactional supporting documentation, must be maintained according to established business processes.

Recording

Gore Partners may use tools (such as Microsoft Teams or other software) to record or transcribe meetings and interactions. Gore Partners must inform participants about the recording or transcribing before the meeting starts, preferably in the meeting invitation, and allow participants to opt-out if they choose. If a meeting recording tool does not show a clear indicator throughout the meeting, the host should notify late joiners that the meeting is being recorded.

For hybrid and automatically recorded meetings, the host should inform all participants about the recording in the meeting invitation or chat. Recordings must be paused during breaks or non-business discussions.

Meetings that involve sensitive personal information or topics should not be recorded. Examples include: patient data, contribution or compensation discussions, Confidential Gore Technology, etc.

Gore AI Tools

Gore Partners are encouraged to utilize Gore AI tools **provided by Gore** to enhance productivity, streamline workflows, and support decision-making processes. When entering company or personal data into Gore AI tools, Gore Partners must ensure that the data is accurate, relevant, and complies with data privacy and security protocols. Gore Partners must not upload or share any data in non-Gore provided AI tools that is confidential, sensitive, proprietary, or protected by regulations unless explicitly authorized by the leader and assessed by Information Security. Additionally, Gore Partners should be aware that AI-generated results can sometimes be misleading or incorrect. Therefore, it is essential to verify the accuracy and reliability of AI outputs before making decisions or taking actions based on them. Gore Partners are

responsible for the outcomes generated by AI tools and should be prepared to explain and justify those outcomes. Misuse of AI tools, such as generating misleading information, violating intellectual property rights, or automating tasks without proper oversight, is strictly prohibited and may result in disciplinary action, up to and including termination of employment.

Compliance and Reporting

- Gore Partners shall complete any training associated with this Policy including the mandatory Privacy and Information Security training.
- Gore Partners who become aware of any actual or suspected security incident or unauthorized use or access to Gore Assets must immediately notify ITAC.
- Violation of this Policy, subject to applicable laws, may result in disciplinary action, up to and including termination of employment and/or legal action where necessary.

Appendix A - Regional Variances

Section 1	Monitoring Information for Italy	Sets forth additional provisions relevant to associates in Italy.

Section 1 – Monitoring Information for Italy

The monitoring activities described in the Policy are performed by Gore only within the limits and according to the modalities set out by Italian employment and privacy law.

First, pursuant to Article 4, par. 1, of Law of 20 May 1970, no. 300, Gore does not perform any of such activity with the purpose of monitoring Associates' activity at the workplace, except as required to comply with the data protection laws of Italy.

Nonetheless, Gore installed Security tools which may trigger the indirect possibility of remotely monitoring the Associates' activity.
Such installation is needed to properly safeguard Gore's organization and Assets. As stated above, it identifies and addresses security, sensitive data leakage, fraud detection, compliance with applicable laws and misuse, which create risk to Gore's organization and assets.

Whenever possible, monitoring is conducted on an automated and/or random basis. Nonetheless, Gore may attempt to identify a Gore Partner if Gore has reason to believe that the Gore Partner committed misconduct and such misconduct may jeopardize Gore's organization, security, or assets.

Appendix B – Information Types, Circumstances and Purposes for Monitoring Gore Partners Activity on Gore Assets.

Section 1: Information that may be captured and logged when monitoring

Network activity, including:

- Date/time
- User ID, device ID, workstation ID, IP address and other unique identifiers
- Physical and logical path of data flows, including Origin and Destination
- Data volume
- Actions
- Key words (such as "confidential", "for internal use only", etc.).

Internet activity, including:

- Date/time
- User ID
- Originating IP address
- Destination address (where permissible)
- Transferred data volume

Incoming and outgoing e-mails:

- Date/time
- Sender and recipient address
- Message ID
- Message size
- Subject
- Sensitive data key words (e.g., “confidential” and “internal use only”, etc.)
- Only for emails that trigger for “Flagged Content”: email body and attachments.

Data loss prevention tools search for key words (such as “Patient ID”) and patterns in data to detect potential leakage of sensitive data (such as customer, healthcare patient or Gore sensitive data). These tools monitor outgoing email and outgoing traffic from laptops, desktops, and cloud usage (traffic to the web, cloud, USB/CD/DVD, printers, and network drives) and flag specified items.

Processed data (that may contain unique user, device, and/or location identifiers) is used only for the following purposes:

- Analysis and correction of technical errors.
- Ensuring system security; including the maintenance of lists of blocked Internet pages ("Block List").
- Optimization and access control of the network.
- Data protection control.

Section 2: Specific Examples of Monitoring and their purpose:

- Protection of Gore Information Assets from unauthorized disclosure, deletion or alteration.
- Compliance with investigation of and enforcement of legal requirements and Gore’s policies.
- Protection of its systems and networks from viruses, Trojans, and other malware.
- Protection of its systems and networks from unauthorized access and/or unauthorized manipulation.
- Protection of the legal rights, security and safety of Gore and others; and
- As otherwise required by law, regulations, court order or the request or requirement of the relevant authorities or law enforcement agencies.